IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FORT MCCLELLAN CREDIT UNION, on behalf of itself and all others similarly situated,	)	
Plaintiff,	)	**CIVIL ACTION NO.:** _____
v.	)	**JURY TRIAL DEMANDED**
EQUIFAX, INC., and EQUIFAX INFORMATION SERVICES LLC,	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Fort McClellan Credit Union ("Plaintiff"), individually and on behalf of similarly situated banks, credit unions and other financial institutions, alleges the following against Equifax, Inc. and Equifax Information Services LLC (collectively "Equifax" or "Defendants"):

SUMMARY OF ACTION

1. Plaintiff brings this class action on its own behalf and on behalf of other financial institutions that have suffered, and continue to suffer, financial losses as a direct result of Equifax's failure to take adequate and reasonable

measures to protect the personal identifying information of some 145.5 million U.S. consumers, credit card numbers of some 209,000 consumers, and dispute information from some 182,000 consumers, that was stored in its data systems (the "Confidential Consumer Data"). The cybersecurity incident during which such Confidential Consumer Data was disclosed by Equifax, which is described in more detail herein, is referred to herein as the "Equifax Data Breach."

2. Despite repeated warnings from security experts about the risk of data breaches and numerous data breaches by multiple companies and even by Equifax competitor Experian, another credit reporting agency, over the past few years, Equifax failed to comply with industry standards and its statutory and common law duties to protect confidential, personal identifying and credit information.

3. On September 7, 2017, Equifax publicly acknowledged a cybersecurity incident / data breach that has potentially impacted some 143 million U.S. consumers, or approximately half of all U.S. consumers who have credit histories. Equifax admitted that it discovered this data breach on July 29, 2017, and that the unauthorized access to Equifax's Confidential Consumer Data began in mid-May 2017. In other words, Equifax's data security was so deficient that they did not realize that their data systems had been hacked for more than two

months, leaving Confidential Consumer Data exposed and accessible before it finally realized a breach had occurred.

4. Rather than timely disclose its data breach, Equifax waited almost six (6) weeks to publicly disclose the occurrence. In the interim, three Equifax executives sold some $1.8 million of Equifax stock. These executives include Chief Financial Officer John Gamble, who sold approximately $946,000 worth of Equifax stock on August 1, 2017; President of United States Information Solutions Joseph Loughran, who sold approximately $584,000 of Equifax stock, also on August 1, 2017; and President of Workforce Solutions Rodolfo Ploder, who sold approximately $250,000 of Equifax stock on August 2, 2017.

5. On October 2, 2017, Equifax disclosed that the Confidential Consumer Data of an additional 2.5 million U.S. consumers had been exposed in the Equifax Data Breach. Thus, some 145.5 million U.S. consumers' Confidential Consumer Data was disclosed by Equifax.

6. As Equifax's CEO admitted: "The company failed to prevent sensitive information from falling into the hands of wrongdoers. . . . [T]he breach occurred because of both human error and technology failures."[1]

7. Plaintiff seeks to recover damages as well as equitable relief on behalf of itself and all other similarly situated financial institutions in the United States.

JURISDICTION AND VENUE

8. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C § 1332(d). The matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, at least one member of the proposed Class is of diverse citizenship from a Defendant, and there are more than 100 putative class members.

9. This Court has personal jurisdiction over Equifax. Defendants were incorporated or formed pursuant to Georgia law, maintain their principal place of

[1] Oversight of the Equifax Data Breach: Answers for Consumers: Hearing before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Prepared Testimony of Richard F. Smith), https://democrats-energycommerce.house.gov/committee-activity/hearings/hearings-on-oversight-of-the-equifax-data-breach-answers-for-consumers.

business in the state of Georgia, regularly conduct business in Georgia, and have sufficient minimum contacts in Georgia.

10. Venue is proper under 18 U.S.C. § 1391(b) because Equifax's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

11. Plaintiff Fort McClellan Credit Union is a credit union with its principal place of business in Anniston, Alabama. Plaintiff was originally chartered in 1953. Plaintiff is a cooperative with some 24,000 of members (who are also consumers) and approximately $230 million in assets.

12. Plaintiff holds consumer deposits, provides consumer loans, processes consumer transactions, issues credit and debit cards to consumers, and has suffered financial losses due to the Equifax Data Breach.

13. Defendant Equifax, Inc. is a Georgia corporation with its principal place of business located at 1550 Peachtree St. NW, H46, Atlanta, Georgia 30309-2402. Equifax, Inc. can be served at this address, via its Registered Agent Shawn Baldwin. Equifax, Inc. is the parent corporation and owns 100% of Equifax Information Services LLC. Equifax is the oldest and second-largest consumer

credit reporting agency in the United States. Equifax, Inc. was founded in 1899, reported $3.1 billion in revenue for 2016, and is publicly traded on the New York Stock Exchange under the ticker symbol "EFX."

14. Defendant Equifax Information Services LLC is a Georgia limited liability company with its principal place of business located at 1550 Peachtree St. NW, H46, Atlanta, Georgia 30309-2402. Equifax Information Services LLC can also be served at this address, via its Registered Agent Shawn Baldwin. It is wholly owned by Equifax, Inc., and both Equifax Defendants acted as agents or the alter-egos of each other in regard to the Equifax Data Breach.

STATEMENT OF FACTS

15. Equifax is one of three major consumer reporting agencies that compiles and maintains files on consumers on a nationwide basis. As such, Equifax also tracks and rates the financial history of U.S. consumers. Equifax stores and maintains a huge amount of credit data regarding U.S. consumers, including, in addition to their personal identifying information (including names, addresses, social security numbers, dates of birth and driver license numbers), account numbers, loan information (including original loan amounts and dates, balances, past due amounts, current status and payment history), credit card

accounts (including credit limit, balances, past due amounts, current status and payment history), as well as information on everything from child support payments, credit limits, missed or past due rent and utilities payments, bankruptcy history, liens, addresses, and employment history. All of this information, and more, factors into credit scores and can and does affect the availability of credit, the terms upon which credit is offered, insurance underwriting decisions, and employment decisions.

16. Equifax gathers and maintains credit-reporting information relating to over 820 million individual consumers and over 91 million businesses. Equifax obtains this data from companies that have extended credit to consumers in the past, currently extend credit to consumers, or who wish to extend credit to consumers. Credit card companies, banks, credit unions, retailers, and auto and mortgage lenders all report the details of consumer credit activity to Equifax.

17. Equifax compiles and analyzes the data that it collects and sells the information in reports designed for: credit services, decision analytics, marketing and consumer assistance.

18. According to Equifax's September 7, 2017 press release, the Equifax Data Breach was discovered on July 29, 2017. The perpetrators gained access by

"[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to retrieve "certain files." In other words, the Equifax Data Breach was the direct result of Equifax's failure to properly secure and protect its U.S. website.

19. Equifax failed to heed warnings from security experts about the vulnerability of the Apache Struts software that it was utilizing on its U.S. website and had failed to update the software to address a known security loophole that had been identified and disclosed prior to the Equifax Data Breach.

20. Included among the Confidential Consumer Data exposed during the Equifax Data Breach was a treasure trove of personal data: names, dates of birth, Social Security numbers and addresses. In some cases – Equifax estimates 209,000 – the breached data also included actual credit card numbers. Documentation about disputes was also leaked, exposing additional personal information of approximately 182,000 American consumers.

21. Unlike data breaches that have affected the customers of certain stores or customers whose credit cards were issued by particular banks, here, many individual consumers affected by the Equifax Data Breach may not even be aware that Equifax has exposed their data via breach. Equifax's data is furnished by

credit card companies, banks, credit unions, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies. In addition, Equifax obtains data published in public records.

22. Financial institutions like Plaintiff are on the front lines following a data breach, notifying consumers and working with them to mitigate damages, crediting accounts for fraudulent charges and increasing security by implementing specific and further identity theft programs.

23. Financial institutions have received Compromised Account Management System ("CAMS") alerts on their members' accounts from VISA. CAMS alerts typically are issued by VISA when there is some event that jeopardizes the security of a financial institution's customers' accounts.

24. Plaintiff has spent time and resources notifying and communicating with its members/customers about the Equifax Data Breach, adding additional fraud oversight, combating fraud attempts on customers' accounts, and helping its members/customers mitigate damages.

25. Confidential Consumer Data like that exposed in the Equifax Data Breach is extremely valuable to cybercriminals, who have capitalized and will, for years, continue to capitalize on it by obtaining unauthorized credit in the names of

injured U.S. consumers, launching targeted phishing campaigns and continuing to sell the Confidential Consumer Data to others for their unauthorized use.

26. Plaintiff has suffered actual injury in that it has been required to incur costs to notify its consumer members/customers that their Confidential Consumer Data, entrusted to Equifax, has been compromised due to the Equifax Data Breach, answering questions and responding to concerns from consumer members/ customers.

27. Plaintiff has further been subjected to an increased number of fraud attempts following the Equifax Data Breach.

28. Further, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud and identity theft posed by the misuse of Confidential Consumer Data to incur fraudulent charges that will have to be credited to consumers whose Confidential Consumer Data was exposed and due to identity theft and the opening of fraudulent accounts.

29. Plaintiff and other financial institutions will, in the end, be obligated to pay the costs of identity theft and fraudulent accounts, as consumer victims will not bear ultimate responsibility for such losses.

30. Moreover, Plaintiff and other financial institutions have a continuing interest in ensuring the integrity of the credit reporting and scoring systems, the integrity of which have been called into question due to the Equifax Data Breach. Accordingly, Plaintiff and those similarly situated have an interest in seeing that Confidential Consumer Data is protected and safeguarded from future breaches.

31. Additionally, because Equifax provides core services to the businesses of extending loans and credit, Plaintiff and other financial institutions are faced with the costs of dealing with customers who have frozen their credit, making it impossible to evaluate their creditworthiness for current or potential credit or loans or to comply with regulatory requirements. Plaintiff and other financial institutions also face the dilemma that, to carry out their business, they must exchange their customers' Confidential Consumer Data with Equifax, which has proven to lack the ability to secure data.

32. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that the Confidential Consumer Data collected, maintained and stored in its computer systems is highly sensitive, susceptible to attack, and could be used by third parties for wrongful purposes, such as identity theft and fraud, and

that financial institutions, like Plaintiff, would suffer significant financial losses as the result of a data breach.

33. It is well known and the subject of many media reports that Confidential Consumer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Equifax competitor Experian, Equifax maintained an insufficient and inadequate system to protect the Confidential Consumer Data of Plaintiff's customers.

34. Confidential Consumer Data is a valuable commodity because it contains not only payment card numbers but personal identifying information as well. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. Personal identifying information is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

35. Legitimate businesses and the criminal underground alike recognize the value in Confidential Consumer Data contained in Equifax's data systems;

otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing Confidential Consumer Data] from 38 million users."

36. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding Confidential Consumer Data and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on financial institutions as a result of a breach.

37. Equifax was, or should have been, fully aware of the significant number of individuals whose Confidential Consumer Data it collected, and thus, the significant number of individuals who would be harmed by a breach of Equifax's systems. Additionally, Equifax knew or should have known that financial institutions, such as Plaintiff, would ultimately suffer the most significant financial losses as a result of fraudulent charges incurred due to the Equifax Data Breach.

38. Equifax was aware of the risk posed by its insecure U.S. website. Equifax was further aware of the extraordinarily sensitive nature of the personal

identifying and account information that it maintains as well as the resulting impact that a data breach would have on financial institutions, including Plaintiff and similarly situated financial institutions or class members.

39. Unfortunately, despite publicly available knowledge of the continued compromises of personal identifying and account information in the hands of unauthorized third parties, Equifax's approach to maintaining the privacy and security of is confidential consumer data, including the data belonging to Plaintiff's customers, was reckless, or at the very least, negligent. Equifax failed to follow industry standards and failed to effectively monitor its security systems to ensure the safety of Confidential Consumer Data. Equifax's substandard and deficient security protocols and failure to adequately monitor for unauthorized intrusion caused Confidential Consumer Data to be compromised for months without even noticing the security failure.

40. The ramifications of Equifax's failure to keep Plaintiff's customers' and Class members' customers' data secure are severe.

41. The Federal Trade Commission (or "FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name

or number that may be used, alone or in conjunction with any other information, to identify a specific person."

42. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

43. Identity thieves can use personal information, including the Confidential Consumer Data exposed in the Equifax Data Breach, which Equifax failed to keep secure, to perpetrate a variety of crimes that harm financial institutions. For instance, identity thieves may commit various types of credit fraud such as: obtaining a driver license or identification card in the victim's name but with another's picture; using the consumer's fraudulently obtained information to clone credit or debit cards or obtain new credit or loans that will never be re-paid, leaving Plaintiff and other financial institutions with substantial bad debt.

44. Javelin Strategy and Research reports that, over the past six years, identity thieves have stolen $112 billion.

45. There may be a time lag between when harm occurs versus when it is discovered, and also between when confidential personal identifying information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

46. The Equifax Data Breach has destabilized and threatens to disrupt the usual business operations of most all financial institutions, which rely upon Equifax to provide services supporting the institutions' core credit and lending functions.

47. Regulators often require the use of credit reports to demonstrate the health of their credit and loan portfolios. Such information will be difficult to obtain because many consumers have implemented credit freezes that eliminate the ability of others to obtain credit reports.

48. Plaintiff and Class members now face years of constant surveillance and increased vigilance against fraudulent account activity involving their

customers and identity theft. The Class is incurring and will continue to incur such damages.

49. The Confidential Consumer Data of Plaintiff's and Class members' customers is private and sensitive in nature and was inadequately protected by Equifax. Equifax's disclosure of Confidential Consumer Data in the Equifax Data Breach was not authorized.

50. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Class members' customers' Confidential Consumer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' customers' Confidential Consumer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

51. Equifax had the resources to prevent a breach, but neglected to adequately implement, monitor, update or maintain data security, despite the increasing number of well-publicized data breaches.

52. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, it could and would have prevented the Equifax Data Breach and prevented the theft of 145.5 million United States consumers, including Plaintiff's and Class members' customers' Confidential Consumer Data.

53. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Equifax Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to expend increased amounts on data security, fraud prevention and investigation, and increased vigilance to mitigate the actual and potential impact of the Equifax Data Breach on their businesses.

54. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' customers' Confidential Consumer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. the costs of notifying their customers of the Equifax Data Breach;

b. the costs of reimbursing unauthorized charges on Plaintiff's customers' (and the customers of class members) debit and credit card accounts;

c. the costs of canceling and reissuing payment cards, changing or closing accounts;

d. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their customers' Confidential Consumer Data being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the black market;

e. the untimely and inadequate notification of the Equifax Data Breach;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Equifax Data Breach, including heightened security and alerts, including additional administrative costs to safeguard the safety of their own data;

g. the costs spent to address, attempt to ameliorate, mitigate and deal with the actual and future consequences of the Equifax Data Breach, including increased security against and investigating fraudulent charges, cancelling customers' cards and accounts and reissuing cards; purchasing

credit monitoring and identity theft protection services for their customers, and the imposition of withdrawal and purchase limits on compromised accounts, among other damages; and

h. lost interest revenue and transaction fees due to reduced payment card usage.

55. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to Confidential Consumer Data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

56. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines state that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to hack the system; watch for large

amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

57. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

58. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

59. Multiple states have enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code § 19.255; or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect Payment Card Data. Banks and other financial institutions are required to notify their customers of data security breaches pursuant to the federal Gramm-Leach-

Bliley Act. Moreover, most states have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

60. Equifax's failure to employ practices and procedures reasonably capable of securing the Payment Card Data of Plaintiff's customers and of the customers of the proposed Class violated all of these statutory and industry-imposed obligations and caused substantial damages to Plaintiff and the proposed Class.

61. Indeed, the fact that confidential personal identifying and account information was left exposed for some 2.5 months, while Equifax continuously failed to detect this vulnerability, demonstrates Equifax's lack of security and safeguards with respect to the confidential personal identifying and account information of Plaintiff's customers and of the class members' customers.

62. Plaintiff and the proposed Class were required to act immediately to mitigate fraudulent transactions from being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud losses, but Plaintiff and the proposed Class

members are not. Financial institutions bear primary responsibility for reimbursing members for fraudulent charges on the payment cards they issue.

63. As a result of the Equifax Data Breach, Plaintiff and the proposed Class have been forced to cancel and reissue payment cards, change or close accounts, notify customers that their accounts and personal identifying information were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and/or take other steps to protect themselves and their members. Plaintiff and the proposed Class have also lost interest and transaction fees due to reduced card usage.

64. The financial damages suffered by Plaintiff and the proposed Class are massive and continue to increase.

65. The Equifax Data Breach caused Plaintiff to incur significant costs associated with, among other things, notifying members of issues related to the data breach, closing out and opening new customer/member accounts, reissuing members' cards, and/or refunding members' losses resulting from the unauthorized use of their accounts.

CLASS ALLEGATIONS

66. Plaintiff brings this action on behalf of itself and all other similarly situated financial institutions pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiff seeks certification of the following proposed Class (the "Class"), defined as:

> All banks, credit unions, and financial institutions in the United States (including its Territories and the District of Columbia) that provide banking products and services to customers and members whose personal information was collected or amassed by Equifax which was compromised in the 2017 breach of Equifax's U.S. website ("The Financial Institutions Class").

67. Excluded from the proposed Class are Equifax, their subsidiaries and affiliates; all Equifax employees; all persons who make a timely election to be excluded from the proposed Class; government entities; the judge to whom this case is assigned, his/her immediate family, and his/her court staff.

68. Plaintiff is a member of the Class. The members of the Class are readily ascertainable, and Equifax likely has contact information that could be used to provide notice to Class members.

69. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of its claims on a class-wide

basis, using the same evidence or types of evidence as would be used in individual action alleging the same claims.

70. Plaintiff reserves the right to modify, expand or amend the class definition and to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate following discovery.

71. Numerosity: All requirements of Fed. R. Civ. P. 23(a)(l) are satisfied. The members of the proposed Class are so numerous and geographically dispersed that individual joinder of all proposed Class members is impracticable. There are over 6,700 FDIC-insured commercial banks in the United States, and thousands of state and federally chartered credit unions, though the precise number of class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

72. Commonality and Predominance: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action

involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

a. Whether Equifax knew or should have known of the susceptibility of its U.S. website to a data breach;

b. Whether Equifax's security measures to protect its U.S. website were reasonable in light of known susceptibilities, FTC data security recommendations and other measures recommended by data security experts;

c. Whether Equifax's conduct resulted in the breach of its U.S. website and the unauthorized disclosure of the Confidential Consumer Data;

d. Whether Equifax's failure to implement adequate data security measures allowed the Equifax Data Breach to occur;

e. Whether reasonable security measures known and recommended by the data security community could have reasonably prevented the Equifax Data Breach;

f. Whether reasonable measures to monitor and detect unauthorized activity known and recommended by the data security community could have discovered or stopped the breach faster than 2.5 months after it began;

g. Whether Equifax's notifications regarding the Equifax Data Breach were timely;

h. Whether Equifax's actions or omissions were negligent;

i. Whether Equifax failed to encrypt sensitive personal identifying and/or account information;

j. Whether Equifax owed a duty to Plaintiff and to the Class;

k. Whether the harm to Plaintiff and the Class were foreseeable;

l. Whether Plaintiff and the Class are entitled to injunctive relief; and

m. Whether Plaintiff and the Class suffered and are entitled to damages.

73. Typicality: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having customers whose personal identifying and account information was compromised in the Equifax Data Breach. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' uniform conduct, as described in detail above. Plaintiff's injuries are akin to those of other Class members' injuries, and Plaintiff seeks relief consistent with the relief sought by the Class. The factual bases of Plaintiff's and the Class' claims are common to all Class members.

74. Adequacy: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type,

and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

75. Superiority: The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

76. Injunctive and Declaratory Relief: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Equifax, through its uniform conduct, acted or refused to act

on grounds generally applicable to the class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

COUNT I

Negligence

77. Plaintiff repeats and re-alleges the factual allegations contained in every preceding paragraph as if fully set forth herein.

78. Equifax owed a duty to Plaintiff and the members of the proposed Class to take reasonable care to protect confidential personal identifying and account information belonging to Plaintiff's and the class members' customers and to timely notify Plaintiff and the proposed Class in the event of a data breach. This duty arises from multiple sources.

79. Equifax further owes a duty to Plaintiff and the proposed Class because it was foreseeable that Defendants' U.S. website and the personal identifying information that it processed would be targeted by hackers. It also was foreseeable that such hackers would extract personal identifying and account information from Defendants' systems and misuse that information to the detriment of Plaintiff and the Class members, and that Plaintiff and the Class would be forced to mitigate such fraud or such potential fraud by notifying its

members and customers that their personal identifying and account information was disclosed, requiring Plaintiff and Class members to cancel payments and accounts, reissue accounts and payment cards, and to reimburse their customers for fraud losses.

80. Defendants' common law duty also arises from the special relationship that existed between Defendants and Plaintiff and the Class. Plaintiff and the Class entrusted Defendants with the personal identifying and account information belonging to the customers of Plaintiff and the Class. Defendants, as the holder and processor of that information, were the only parties who realistically could ensure that its U.S. website systems were sufficient to protect the sensitive personal identifying and account information it was entrusted to process and/or hold.

81. Section 5 of the FTCA, 15 U.S.C. § 45, further required Equifax to take reasonable measures to protect the Confidential Consumer Data. Section 5 prohibits unfair practices in or affecting commerce, which requires and obligates Defendants to take reasonable measures to protect any personal identifying or account information may hold or process. The FTC publications and data security breach orders described above further form the basis of Defendants' duty. In

addition, individual states have enacted statutes based upon the FTCA that also created a duty.

82. In sum, Equifax owed a duty to Plaintiff and to the Class to adequately secure consumers' personal identifying and account information.

83. Equifax, by its actions and omissions, breached its duties to Plaintiff and the Class. The specific negligent acts and omissions committed by Defendants include, but are not limited to, some or all of the following:

a. failure to properly secure their U.S. website;

b. failure to update and plug known security vulnerabilities in software they utilized;

c. failure to track and monitor access to their U.S. website and sensitive consumer personal identifying and account data;

d. failure to limit access to their network and to sensitive consumer personal identifying and account information to those with a valid purpose;

e. failure to encrypt sensitive consumer personal identifying and account data;

f. failure to implement adequate data security measures;

g. failure to recognize red flags signaling that Defendants' systems were inadequate, and that as a result, the potential for a massive data breach was increasingly likely;

h. failure to recognize that hackers were stealing sensitive consumer personal identifying and account data while the data breach was taking place; and

i. failure to disclose the Equifax Data Breach in a timely manner.

84. In connection with the conduct described above, Equifax acted wantonly, recklessly, and with complete disregard for the consequences.

85. Equifax knew or should have known of the risks associated with the vulnerabilities of its U.S. website and data systems.

86. Equifax knew or should have known that its failure to take reasonable measures to secure its U.S. website and data systems against obvious risks would result in harm to Plaintiff and to the Class.

87. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to canceling and reissuing payment cards, changing or closing accounts, notifying customers that their sensitive personal identifying and account information was

compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, implementing additional fraud monitoring and protection measures, investigating potentially fraudulent activity, indemnifying customers for fraudulent charges, unwinding or absorbing charges to new accounts opened by identity thieves, and/or taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach.

COUNT II

Negligence *Per Se*

88. Plaintiff repeats and re-alleges the factual allegations contained in every preceding paragraph as if fully set forth herein.

89. Equifax's failure to use reasonable measures to protect sensitive consumer personal identifying and account information violates section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair…practices in or affecting commerce" in the United States. The FTC publications and orders described above also form the basis of Defendants' duty.

90. Defendants violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect sensitive consumer personal

identifying and account information and not complying with applicable industry standards, as previously described in detail. Defendants' conduct was particularly unreasonable given the nature and amount of sensitive consumer personal identifying and account information it obtained, processed, and/or stored and the foreseeable consequences of a data breach at a nationwide credit reporting agency, including, specifically, the immense damages that would result to consumers and financial institutions.

91. The FTC has interpreted Section 5 of the FTCA to include the unfair practice of failing to maintain reasonable security to protect sensitive or personal consumer information.

92. Defendants' violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence per se.

93. Plaintiff and the proposed Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiff and many class members are credit unions, which are organized as cooperatives whose members are consumers.

94. Moreover, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused similar harm suffered by Plaintiff and the proposed Class.

95. As a direct and proximate result of Defendants' negligence per se, the Plaintiff and the Class have suffered and continue to suffer injury, including, but not limited to, the expenses of notifying customers that their sensitive personal identifying and account information has been breached, cancelling and reissuing payment cards, changing or closing accounts, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring, and/or taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach.

COUNT III

Declaratory and Injunctive Relief

96. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

97. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain tortious acts that violate the terms of the federal and state statutes described herein.

98. An actual controversy has arisen in the wake of the Equifax Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to safeguarding the sensitive personal identifying and account information of Plaintiff's and the Class members' customers. Defendants' actions in this respect were inadequate, and Defendants deny such allegations. Additionally, Plaintiff continues to suffer injury as additional fraudulent activity will continue, unabated, while the information sufficient to steal and clone the identities of customers of Plaintiff and the Class remain available to be used in the future.

99. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed and continue to owe a legal duty to secure the sensitive personal identifying and account information of Plaintiff's and the Class members' customers, specifically

including the Confidential Consumer Data previously disclosed in the Equifax Data Breach;

b. Defendants breached this legal duty by failing to employ reasonable measures to secure the sensitive personal identifying and account information of Plaintiff's and the Class members' customers;

c. Defendants' breach of their legal duty proximately caused the data breach; and

d. Banks, credit unions, and other financial institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Defendants' data breach were damaged and are legally entitled to recover the costs they incurred from Defendants.

100. Plaintiff and the Class are also entitled to corresponding injunctive relief requiring Defendants to employ adequate security protocols, consistent with industry standards, to protect Plaintiff's and the Class's customers' Payment Card Data. Specifically, this injunction should, among other things, require Defendants to:

a. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. consistent with industry standards, engage third-party auditors to test its systems for weakness and upgrade any such weakness found;

d. audit, test, and train its data security personnel regarding new or modified procedures and how to respond appropriately to a data breach;

e. regularly test its systems for security vulnerabilities, consistent with industry standards;

f. timely notify Plaintiff, the Class and consumers in the event of any future data breach; and

g. timely implement all upgrades and patches recommended by manufacturers of security software and firewalls used by Defendants.

101. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendants' data systems. The risk of another such data breach is real, immediate, and substantial. If another breach of Defendants' data systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

102. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if Defendants suffer another massive data breach, Plaintiff and the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable data security

measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

103. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing (or at least minimizing) another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and on behalf of the proposed Class, requests that this Court award relief against Defendants as follows:

a. Providing a jury trial for all issues so triable;

b. Entering an order certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;

c. Awarding Plaintiff and the Class members compensatory damages with pre-judgment and post-judgment interest;

d. Entering a declaratory judgment in favor of Plaintiff and the Class as described above;

e. Granting Plaintiff and the Class the injunctive relief requested above;

f. Awarding attorneys' fees and costs; and

g. Awarding such other and further relief as the Court may deem necessary or appropriate.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: December 7, 2017 Respectfully submitted,

/s/ Michael L. McGlamry
Michael L. McGlamry
GA Bar 492515
N. Kirkland Pope
GA Bar No. 584255
POPE McGLAMRY, P.C.
3391 Peachtree Road, NE, Suite 300
Atlanta, GA 30326
Tel: (404) 523-7706
Fax (404) 524-1648
E-mail: efile@pmkm.com

Chris T. Hellums (ASB-5583-L73C)
(Pro Hac Application to be Submitted)
Jonathan S. Mann (ASB-1083-A36M)
(Pro Hac Application to be Submitted)
PITTMAN DUTTON & HELLUMS, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
Email: chrish@pittmandutton.com
Email: jonm@pittmandutton.com

Attorneys for Plaintiff